

## ON DEDEKIND'S CRITERION AND MONOGENICITY OVER DEDEKIND RINGS

M. E. CHARKANI and O. LAHLOU

Received 29 November 2002

We give a practical criterion characterizing the monogenicity of the integral closure of a Dedekind ring  $R$ , based on results on the resultant  $\text{Res}(P, P_i)$  of the minimal polynomial  $P$  of a primitive integral element and of its irreducible factors  $P_i$  modulo prime ideals of  $R$ . We obtain a generalization and an improvement of the Dedekind criterion (Cohen, 1996) and we give some applications in the case where  $R$  is a discrete valuation ring or the ring of integers of a number field, generalizing some well-known classical results.

Mathematics Subject Classification: 11Y40, 13A18, 13F30.

**1. Introduction.** Let  $K$  be an algebraic number field and let  $O_K$  be its ring of integers. If  $O_K = \mathbb{Z}[\theta]$  for some number  $\theta$  in  $O_K$ , we say that  $O_K$  has a power basis or  $O_K$  is monogenic. The question of the existence of a power basis was originally examined by Dedekind [5]. Several number theorists were interested in and attracted by this problem (see [7, 8, 9]) and noticed the advantages of working with monogenic number fields. Indeed, for a monogenic number field  $K$ , in addition to the ease of discriminant computations, the factorization of a prime  $p$  in  $K/\mathbb{Q}$  can be found most easily (see [4, Theorem 4.8.13, page 199]). The main result of this paper is [Theorem 2.5](#) which characterizes the monogenicity of the integral closure of a Dedekind ring. More precisely, let  $R$  be a Dedekind domain,  $K$  its quotient field,  $L$  a finite separable extension of degree  $n$  of  $K$ ,  $\alpha$  a primitive element of  $L$  integral over  $K$ ,  $P(X) = \text{Irrd}(\alpha, K)$ ,  $m$  a maximal ideal of  $R$ , and  $O_L$  the integral closure of  $R$  in  $L$ . Assume that  $\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X)$  in  $(R/m)[X]$  with  $e_i \geq 2$ , and let  $P_i(X) \in R[X]$  be a monic lifting of  $\bar{P}_i(X)$  for  $1 \leq i \leq r$ . Then we prove that  $O_L = R[\alpha]$  if and only if, for every maximal ideal  $m$  of  $R$  and  $i \in \{1, \dots, r\}$ ,  $v_m(\text{Res}(P_i, P)) = \deg(P_i)$ , where  $v_m$  is the  $m$ -adic discrete valuation associated to  $m$ . This leads to a necessary and sufficient condition for a simple extension  $R[\alpha]$  of a Dedekind ring  $R$  to be Dedekind. At the end, we give two illustrations of this criterion. In the second example, we give the converse which was not known yet.

**2. Monogenicity over a Dedekind ring.** Throughout this paper  $R$  is an integral domain,  $K$  its quotient field,  $L$  is a finite separable extension of degree  $n$  of  $K$ ,  $\alpha$  is a primitive element of  $L$  integral over  $R$ ,  $P(X) = \text{Irrd}(\alpha, K)$ ,  $m$  is

a maximal ideal of  $R$ , and  $O_L$  is the integral closure of  $R$  in  $L$ . Let  $f$  and  $g$  be two polynomials over  $R$ ; the resultant of  $f$  and  $g$  will be denoted by  $\text{Res}(f, g)$  (see [11]).

**DEFINITION 2.1.** If  $O_L = R[\theta]$  for some number  $\theta \in O_L$ , then  $O_L$  has a power basis or  $O_L$  is monogenic.

**PROPOSITION 2.2.** Let  $R$  be an integrally closed ring and let  $\alpha$  be an integral element over  $R$ . Then  $(R[\alpha])_p = R_p[\alpha]$  for every prime ideal  $p$  of  $R$ . In particular,  $O_L = R[\alpha]$  if and only if  $R_p[\alpha]$  is integrally closed for every prime ideal  $p$  of  $R$  if and only if  $R[\alpha]$  is integrally closed.

**PROOF.** We obtain the result from the isomorphism  $R[\alpha] \simeq R[X]/\langle P(X) \rangle$ , the properties of an integrally closed ring and its integral closure, and the properties of a multiplicative closed subset of a ring  $R$ , notably,  $S^{-1}(R[X]) = (S^{-1}R)[X]$  (see [1]).  $\square$

**DEFINITION 2.3.** Let  $R$  be a discrete valuation ring (DVR),  $p = \pi R$  its maximal ideal, and  $\alpha$  an integral element over  $R$ . Let  $P$  be the minimal polynomial of  $\alpha$ , and  $\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X)$  the decomposition of  $\bar{P}$  into irreducible factors in  $(R/p)[X]$ . Set

$$\begin{aligned} f(X) &= \prod_{i=1}^r P_i(X) \in R[X], \\ h(X) &= \prod_{i=1}^r P_i^{e_i-1}(X) \in R[X], \\ T(X) &= \frac{P(X) - \prod_{i=1}^r P_i^{e_i}(X)}{\pi} \in R[X], \end{aligned} \tag{2.1}$$

where  $P_i(X) \in R[X]$  is a monic lifting of  $\bar{P}_i(X)$ , for  $1 \leq i \leq r$ . We will say that  $R[\alpha]$  is  $p$ -maximal if  $(\bar{f}, \bar{T}, \bar{h}) = 1$  in  $(R/p)[X]$  (where  $(\cdot, \cdot)$  denotes the greatest common divisor (gcd)). If  $R$  is a Dedekind ring and  $p$  is a prime ideal of  $R$ , then we say that  $R[\alpha]$  is  $p$ -maximal if  $R_p[\alpha]$  is  $pR_p$ -maximal.

**REMARKS 2.4.** (1) If  $\pi$  is unramified in  $R[\alpha]$ , that is,  $e_i = 1$  for all  $i$ , then  $\bar{h} = \bar{1}$  and therefore  $R[\alpha]$  is  $p$ -maximal.

(2) Let  $\pi$  be ramified in  $R[\alpha]$ , that is, there is at least one  $i$  such that  $e_i \geq 2$ . Let  $S = \{i \in \{1, \dots, r\} \mid e_i \geq 2\}$  and  $f_1(X) = \prod_{i \in S} P_i(X) \in R[X]$ . Then  $(\bar{f}_1, \bar{T}) = (\bar{T}, \bar{f}, \bar{h})$  in  $(R/p)[X]$  since  $\bar{f}_1 = (\bar{f}, \bar{h})$ . In particular, if every  $e_i \geq 2$ , then  $(\bar{f}, \bar{T}) = (\bar{T}, \bar{f}, \bar{h})$ , because  $\bar{f}$  divides  $\bar{h}$  in this case.

(3) Definition 2.3 is independent of the choice of the monic lifting of the  $\bar{P}_i$ . More precisely, let

$$\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X) = \prod_{i=1}^r \bar{Q}_i^{e_i}(X) \quad \text{with } \bar{P}_i(X) = \bar{Q}_i(X) \text{ for } 1 \leq i \leq r \text{ in } (R/p)[X]. \tag{2.2}$$

Set

$$\begin{aligned}
 g(X) &= \prod_{i=1}^r Q_i(X) \in R[X], & k(X) &= \prod_{i=1}^r Q_i^{e_i-1}(X) \in R[X] \\
 U(X) &= \pi^{-1} \left( P(X) - \prod_{i=1}^r Q_i^{e_i}(X) \right) \in R[X].
 \end{aligned}
 \tag{2.3}$$

Then  $(\bar{f}, \bar{T}, \bar{h}) = 1$  in  $(R/\mathfrak{p})[X]$  if and only if  $(\bar{g}, \bar{U}, \bar{k}) = 1$  in  $(R/\mathfrak{p})[X]$ . Indeed, we may assume that  $R$  is a DVR and  $\mathfrak{p} = \pi R$ . Let  $V_1 = (g - f)/\pi$  and  $V_2 = (k - h)/\pi$ . Then  $\pi T = \pi U + gk - fh$ . Replacing  $g$  by  $\pi V_1 + f$  and  $k$  by  $\pi V_2 + h$ , we find that  $\bar{T} = \bar{U} + \bar{V}_1 \bar{h} + \bar{V}_2 \bar{f}$  and therefore  $(\bar{T}, \bar{f}, \bar{h}) = (\bar{U}, \bar{f}, \bar{h}) = (\bar{U}, \bar{g}, \bar{k})$  since  $\bar{f} = \bar{g}$  and  $\bar{h} = \bar{k}$ .

**THEOREM 2.5.** *Let  $R$  be a Dedekind ring. Let  $P$  be the minimal polynomial of  $\alpha$ , and assume that for every prime ideal  $\mathfrak{p}$  of  $R$ , the decomposition of  $\bar{P}$  into irreducible factors in  $(R/\mathfrak{p})[X]$  verifies:*

$$\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X) \in (R/\mathfrak{p})[X]
 \tag{2.4}$$

with  $e_i \geq 2$  for  $i = 1, \dots, r$  and  $P_i(X) \in R[X]$  be a monic lifting of the irreducible factor  $\bar{P}_i$  for  $i = 1, \dots, r$ . Then  $O_L = R[\alpha]$  if and only if  $v_{\mathfrak{p}}(\text{Res}(P_i, P)) = \deg(P_i)$  for every prime ideal  $\mathfrak{p}$  of  $R$  and for every  $i = 1, \dots, r$ , where  $v_{\mathfrak{p}}$  is the  $\mathfrak{p}$ -adic discrete valuation associated to  $\mathfrak{p}$ .

For the proof we need the following two lemmas.

**LEMMA 2.6.** *Let  $\mathfrak{p} = uR + vR$  be a maximal ideal of a commutative ring  $R$ . Then  $\mathfrak{p}R_{\mathfrak{p}} = vR_{\mathfrak{p}}$  if and only if there exist  $a, b \in R$  such that  $u = au^2 + bv$ .*

**PROOF.** If  $\mathfrak{p}R_{\mathfrak{p}} = vR_{\mathfrak{p}}$ , then there exist  $s \in R$  and  $t \in R - \mathfrak{p}$  such that  $tu = vs$ . Since  $\mathfrak{p}$  is maximal in  $R$ , so there exists  $t' \in R$  such that  $tt' - 1 \in \mathfrak{p}$ . Hence  $u - utt' = u - vst' \in \mathfrak{p}^2$  and there exist  $a, b \in R$  such that  $u = au^2 + bv$ . Conversely,  $u^2R + vR \subseteq vR + \mathfrak{p}^2 \subseteq \mathfrak{p}$ . If there exist  $a, b \in R$  such that  $u = au^2 + bv$ , then  $\mathfrak{p} = u^2R + vR$  and therefore  $vR + \mathfrak{p}^2 = \mathfrak{p}$ . Localizing at  $\mathfrak{p}$  and applying Nakayama's lemma, we find that  $\mathfrak{p}R_{\mathfrak{p}} = vR_{\mathfrak{p}}$ .  $\square$

**LEMMA 2.7.** *Let  $R$  be a commutative integral domain, let  $K$  be its quotient field, and consider  $P, g, h, T \in R[X]$ . If  $g$  is monic and  $P = gh + \pi T$ , then  $\text{Res}(g, P) = \pi^{\deg(g)} \text{Res}(g, T)$ . In particular, if  $\mathfrak{m} = \pi R$  is a maximal ideal of  $R$  and if  $\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X)$  is the decomposition of  $\bar{P}$  into irreducible factors in  $(R/\mathfrak{m})[X]$ , with  $P_i(X) \in R[X]$  a monic lifting of  $\bar{P}_i(X)$  for  $1 \leq i \leq r$ , and  $T(X) = \pi^{-1}(P(X) - \prod_{i=1}^r P_i^{e_i}(X)) \in R[X]$ , then*

$$\text{Res}(P_i, P) = \pi^{\deg(P_i)} \text{Res}(P_i, T)
 \tag{2.5}$$

and  $(\bar{P}_i, \bar{T}) = 1$  in  $(R/m)[X]$  if and only if

$$\text{Res}(P_i, T) = \frac{\text{Res}(P_i, P)}{\pi^{\deg(P_i)}} \in R - m. \quad (2.6)$$

**PROOF.** Let  $x_1, \dots, x_m$  be the roots of  $g$  in the algebraic closure  $\bar{K}$  of  $K$ . It is then easy to see (see [11]) that  $\text{Res}(g, P) = \prod_{i=1}^m P(x_i) = \pi^{\deg(g)} \text{Res}(g, T)$  because  $P(x_i) = \pi T(x_i)$ . The second result follows from  $\text{Res}(\bar{P}_i, \bar{P}) = \overline{\text{Res}(P_i, P)}$  and [2, Corollary 2, page 73].  $\square$

**PROOF OF THEOREM 2.5.** By Proposition 2.2, we may assume that  $R$  is a DVR. Let  $p$  be a prime ideal of  $R$  and  $(O_L)_{(p)}$  the integral closure of  $R_p$  in  $L$ . Let  $\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X)$  in  $(R_p/pR_p)[X]$  with  $e_i \geq 2$  and  $P_i(X) \in R_p[X]$  a monic lifting of  $\bar{P}_i(X)$  for  $1 \leq i \leq r$ . Let

$$T(X) = \frac{P(X) - \prod_{i=1}^r P_i^{e_i}(X)}{\pi} \in R_p[X] \quad (2.7)$$

with  $\pi R_p = pR_p$ .

(a) We prove that if  $(\bar{P}_i, \bar{T}) = 1$  in  $(R_p/pR_p)[X]$  for every  $i = 1, \dots, r$ , then  $(O_L)_{(p)} = R_p[\alpha] = A$ . Indeed,  $\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X)$  in  $(R_p/pR_p)[X]$  and  $R_p$  is a local ring, so by [14, Lemma 4, page 29] (see also [3]) the ideals  $\mathcal{B}_i = \pi A + P_i(\alpha)A$  ( $i = 1, \dots, r$ ) are the only maximal ideals of  $A$ , so  $A$  is integrally closed if and only if  $\mathcal{A}_{\mathcal{B}_i}$  is integrally closed for every  $i = 1, \dots, r$ . More generally, we prove that every  $\mathcal{A}_{\mathcal{B}_i}$  is a DVR. Since  $R_p$  is Noetherian, so  $R_p[\alpha] \simeq R_p[X]/\langle P(X) \rangle$  is Noetherian, hence  $\mathcal{A}_{\mathcal{B}_i}$  is Noetherian since  $\mathcal{A}_{\mathcal{B}_i}$  is a local integral domain with maximal ideal  $\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i}$ . It remains to show that  $\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i}$  is principal. Indeed,  $(\bar{P}_i, \bar{T}) = 1$  in  $(R_p/pR_p)[X]$ , hence there exist polynomials  $U_1, U_2, U_3 \in R_p[X]$  such that  $1 = U_1(X)P_i(X) + U_2(X)T(X) + \pi U_3(X)$ . Now  $P(\alpha) = 0 = \prod_{j=1}^r P_j^{e_j}(\alpha) + \pi T(\alpha)$ , hence  $\prod_{j=1}^r P_j^{e_j}(\alpha) = -\pi T(\alpha)$ , so

$$\begin{aligned} \pi &= \pi U_1(\alpha)P_i(\alpha) + \pi^2 U_3(\alpha) - \prod_{j=1}^r P_j^{e_j}(\alpha)U_2(\alpha) \\ &= \pi^2 U_3(\alpha) + P_i(\alpha)U_4(\alpha) \end{aligned} \quad (2.8)$$

with  $U_4 = \pi U_1 - P_i^{e_i-1}(\prod_{j=1, j \neq i}^r P_j^{e_j})U_2 \in R_p[X]$ . It follows from Lemma 2.6 that  $\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i} = P_i(\alpha) \mathcal{A}_{\mathcal{B}_i}$ , in other words,  $\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i}$  is principal. We conclude that  $\mathcal{A}_{\mathcal{B}_i}$  is a DVR and therefore an integrally closed ring, and  $(O_L)_{(p)} = R_p[\alpha]$ .

(b) We will now prove that  $(\bar{P}_i, \bar{T}) = 1$  in  $(R_p/pR_p)[X]$  for every  $i = 1, \dots, r$  if  $(O_L)_{(p)} = R_p[\alpha]$ . We first show that the ring  $\mathcal{A}_{\mathcal{B}_i}$  is a DVR, for every  $i$ . Indeed,  $R_p$  is a Dedekind ring and  $L$  is a finite extension of  $K$ , and it follows from [10, Theorem 6.1, page 23] that  $(O_L)_{(p)} = R_p[\alpha] = A$  is a Dedekind ring, so  $\mathcal{A}_{\mathcal{B}_i}$  is a DVR. Let us show next that  $T(\alpha)$  is a unit in every  $\mathcal{A}_{\mathcal{B}_i}$ . Indeed,  $\mathcal{A}_{\mathcal{B}_i}$  is a DVR and so its maximal ideal  $\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i} = \pi \mathcal{A}_{\mathcal{B}_i} + P_i(\alpha) \mathcal{A}_{\mathcal{B}_i}$  is principal. Let  $\lambda \in \mathcal{A}_{\mathcal{B}_i}$  be a generator of  $\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i}$ . Then there exist  $u, v \in \mathcal{A}_{\mathcal{B}_i}$  such that  $\lambda = \pi u + P_i(\alpha)v \in \mathcal{B}_i \mathcal{A}_{\mathcal{B}_i} - (\mathcal{B}_i \mathcal{A}_{\mathcal{B}_i})^2$ . Now  $R_p$  is a DVR,  $P = \text{Irrd}(\alpha, R_p)$ ,  $\bar{P} = \prod_{j=1}^r \bar{P}_j^{e_j}$

in  $(R_p/\pi R_p)[X]$ ,  $\pi R_p \in \text{Spec } R_p$ , and  $(O_L)_{(p)} = R_p[\alpha] = A$  is the integral closure of  $R_p$  in  $L = K(\alpha)$  with  $K = \text{Fr}(R_p)$ , and we find that  $\pi A = \prod_{j=1}^r \mathfrak{B}_j^{e_j}$ . Hence  $\pi \in \mathfrak{B}_i^2$  because  $e_i \geq 2$ . Now  $\lambda \notin (\mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i})^2$ , hence  $P_i(\alpha) \notin (\mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i})^2$ , because  $\lambda = u\pi + P_i(\alpha)v$ . It then follows that  $P_i(\alpha)$  is a generator of  $\mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i} = P_i(\alpha) \mathcal{A}_{\mathfrak{B}_i}$  since  $\pi \mathcal{A}_{\mathfrak{B}_i} = (\mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i})^{e_i} = P_i^{e_i}(\alpha) \mathcal{A}_{\mathfrak{B}_i}$ , and  $\pi = P_i^{e_i}(\alpha)\epsilon_1$  with  $\epsilon_1 \in U(\mathcal{A}_{\mathfrak{B}_i})$ . We now show that  $P_j(\alpha) \in U(\mathcal{A}_{\mathfrak{B}_i})$  for every  $j \neq i$ . Indeed, if  $P_j(\alpha) \in \mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i}$ , then there exists  $a_i \in \mathfrak{B}_i$  and  $b_i \in A - \mathfrak{B}_i$  such that  $P_j(\alpha) = a_i/b_i$ . Then  $a_i = P_j(\alpha)b_i \in \mathfrak{B}_i$ . Now,  $\mathfrak{B}_i$  is a prime ideal of  $A$ , hence  $P_j(\alpha) \in \mathfrak{B}_i$ . As  $\mathfrak{B}_j = \pi A + P_j(\alpha)A$ , so  $\mathfrak{B}_j \subset \mathfrak{B}_i$ . The ideal  $\mathfrak{B}_j$  is a maximal ideal of  $A$ , so  $\mathfrak{B}_i = \mathfrak{B}_j$ . This is impossible because the  $\mathfrak{B}_i$  are distinct, and it follows that  $P_j(\alpha) \in U(\mathcal{A}_{\mathfrak{B}_i})$  for every  $j \neq i$ . Thus there exists  $\epsilon_2 \in U(\mathcal{A}_{\mathfrak{B}_i})$  such that  $\prod_{j=1, j \neq i}^r P_j^{e_j}(\alpha) = \epsilon_2$ . Since  $\prod_{j=1}^r P_j^{e_j}(\alpha) = -\pi T(\alpha)$ ,  $\pi = P_i^{e_i}(\alpha)\epsilon_1$ , and  $\prod_{j=1, j \neq i}^r P_j^{e_j}(\alpha) = \epsilon_2$ , then  $T(\alpha) = -\epsilon_2 \epsilon_1^{-1} \in U(\mathcal{A}_{\mathfrak{B}_i})$ . So  $T(\alpha) \in U(\mathcal{A}_{\mathfrak{B}_i})$  for every  $i$ , and  $T(\alpha) \in U(A)$ ; otherwise, Krull's theorem implies the existence of a maximal ideal  $\mathfrak{B}_i$  of  $A$  such that  $T(\alpha) \in \mathfrak{B}_i$ , and  $T(\alpha) \in \mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i} = \mathcal{A}_{\mathfrak{B}_i} - U(\mathcal{A}_{\mathfrak{B}_i})$ , which is impossible. We conclude that  $T(\alpha)$  is a unit in  $R_p[\alpha]$ , and, by [2, Corollary 1, page 73], there exist  $U_1, V_1 \in R_p[X]$  such that  $1 = U_1(X)P(X) + V_1(X)T(X)$ . Consequently  $\bar{1} = \bar{U}_1(X)\bar{P}(X) + \bar{V}_1(X)\bar{T}(X)$  in  $(R_p/\pi R_p)[X]$ , which is principal. Hence  $(\bar{P}, \bar{T}) = 1$  in  $(R_p/\pi R_p)[X]$  since  $\bar{P} = \prod_{i=1}^r \bar{P}_i^{e_i}$  in  $(R_p/\pi R_p)[X]$  then  $(\bar{P}_i, \bar{T}) = 1$  in  $(R_p/\pi R_p)[X]$  for every  $i$ . Our result now follows from Proposition 2.2 and Lemma 2.7. □

**REMARKS 2.8.** (1) Let  $\pi$  be ramified in  $R[\alpha]$ ,  $S = \{i \in \{1, \dots, r\} \mid e_i \geq 2\}$ , and  $f_1(X) = \prod_{i \in S} P_i(X) \in R[X]$ . It follows from Lemma 2.7 that the following statements are equivalent:

- (i)  $(\bar{f}_1, \bar{T}) = 1$  in  $(R/p)[X]$ ;
- (ii)  $v_p(\text{Res}(f_1, P)) = \deg(f_1)$ ;
- (iii) for every  $i \in S$ , we have  $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ , where  $v_p$  is the  $p$ -adic discrete valuation associated to  $p$ .

(2) It follows from the above equivalence and Remark 2.4(2) and (3) that the condition in Theorem 2.5 is independent of the choice of the monic lifting of  $\bar{P}_i$ . More precisely, if  $e_i \geq 2$  for every  $i$ , and if we take another monic lifting  $Q_i$  of  $\bar{P}_i$ , then  $v_p(\text{Res}(P_i, P)) = \deg(P_i)$  for all  $i = 1, \dots, r$  if and only if  $v_p(\text{Res}(Q_i, P)) = \deg(Q_i)$  for all  $i = 1, \dots, r$ .

(3) Theorem 2.5 states that, under the assumption that  $e_i \geq 2$  for every  $i$ ,  $O_L = R[\alpha]$  if and only if  $R[\alpha]$  is  $p$ -maximal for every prime ideal  $p$  of  $R$ .

**COROLLARY 2.9.** Under the assumptions of Theorem 2.5, if  $O_L = R[\alpha]$ , then, for every prime ideal  $p$  of  $R$ ,  $R_p[\alpha]$  is principal and  $\mathfrak{B}_i = P_i(\alpha)R_p[\alpha]$  for every  $i$ .

**PROOF.** Indeed, a Dedekind ring having only a finite number of prime ideals is principal. To prove the second statement, take  $x \in A$  such that  $\mathfrak{B}_i = xA$ . Then  $\mathfrak{B}_i \mathcal{A}_{\mathfrak{B}_i} = x \mathcal{A}_{\mathfrak{B}_i} = P_i(\alpha) \mathcal{A}_{\mathfrak{B}_i}$ , hence  $P_i(\alpha) = x\epsilon$  with  $\epsilon \in U(\mathcal{A}_{\mathfrak{B}_i})$ . Then  $\epsilon \in U(A)$ , so  $\mathfrak{B}_i = P_i(\alpha)A$ . □

**DEFINITION 2.10.** Let  $R$  be a DVR with maximal ideal  $m = \pi R$ , with  $f, g \in R[X]$  monic polynomials. Then  $f$  is called an Eisenstein polynomial relative to  $g$  if there exists  $T \in R[X]$  and an integer  $e \geq 1$  such that  $f = g^e + \pi T$  and  $(\bar{g}, \bar{T}) = 1$  in  $(R/\pi R)[X]$ .

**REMARK 2.11.** As in the classical Eisenstein's criterion, we have a criterion for the irreducibility of an Eisenstein polynomial relative to  $g$ , called the Schönemann criterion, see [12, page 273]; if  $f = g^e + \pi T$  is an Eisenstein polynomial relative to  $g$  such that  $\bar{g} \in (R/m)[X]$  is irreducible and  $\deg(T) < e \deg(g)$ , then  $f$  is irreducible in  $K[X]$ .

**COROLLARY 2.12.** Let  $R$  be a DVR with maximal ideal  $m = \pi R$ . If  $\bar{P} = \bar{g}^e$  in  $(R/m)[X]$  with  $e \geq 2$ , then  $O_L = R[\alpha]$  if and only if  $P$  is an Eisenstein polynomial relative to  $g$ .

**PROOF.** We obtain the result using Theorem 2.5, Definition 2.10, and Lemma 2.7. □

**REMARK 2.13.** Corollary 2.12 generalizes [14, Propositions 15 and 17]; it integrates the two results in one statement and provides the converse.

**3. Monogenicity over the ring of integers.** Let  $K = \mathbb{Q}(\alpha)$  be a number field of degree  $n$ ,  $P(X) \in \mathbb{Z}[X]$  a minimal polynomial of  $\alpha$ ,  $O_K$  the ring of integers of  $K$ , and  $p$  a prime number.

**PROPOSITION 3.1.** Let  $K = \mathbb{Q}(\alpha)$  be a number field and  $P$  the minimal polynomial of  $\alpha$ . Then  $O_K = \mathbb{Z}[\alpha]$  if and only if for every prime number  $p$  such that  $p^2$  divides  $\text{Disc}(P)$ , the prime number  $p$  does not divide  $\text{Ind}(\alpha)$ .

**PROOF.** We obtain the result from the fact that  $O_K = \mathbb{Z}[\alpha]$  if and only if  $\text{Ind}(\alpha) = 1$ , and  $\text{Disc}(P) = (\text{Ind}(\alpha))^2 d_K$  (see [6], [4, page 166]). □

**PROPOSITION 3.2.** Let  $\bar{P}(X) = \prod_{i=1}^r \bar{P}_i^{e_i}(X)$  be the factorization of  $P(X)$  modulo  $p$  in  $\mathbb{F}_p[X]$ , and put  $f(X) = \prod_{i=1}^r P_i(X)$  with  $P_i(X) \in \mathbb{Z}[X]$  a monic lifting of  $\bar{P}_i(X)$  and  $e_i \geq 2$  for all  $i$ . Let  $h(X) \in \mathbb{Z}[X]$  be a monic lifting of  $\bar{P}(X)/\bar{f}(X)$  and  $T(X) = (f(X)h(X) - P(X))/p \in \mathbb{Z}[X]$ . Then the following statements are equivalent:

- (i)  $p$  does not divide  $\text{Ind}(\alpha) = [O_K : \mathbb{Z}[\alpha]]$ ;
- (ii)  $(\bar{f}, \bar{T}) = 1$  in  $\mathbb{F}_p[X]$ ;
- (iii)  $v_p(\text{Res}(f, P)) = \deg(f)$ ;
- (iv)  $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ , for every  $i \in \{1, \dots, r\}$ .

**PROOF.** (i)  $\Leftrightarrow$  (ii). Let  $(O_K)_{(p)}$  be the integral closure of  $\mathbb{Z}_{(p)}$  in  $K$ . We first show that  $p$  does not divide  $\text{Ind}(\alpha)$  if and only if  $(O_K)_{(p)} = \mathbb{Z}_{(p)}[\alpha]$ . By the finiteness theorem [13, page 48],  $(O_K)_{(p)} = \bigoplus_{i=0}^{n-1} \mathbb{Z}_{(p)} x_i$ , and, because  $\mathbb{Z}_{(p)}$  is principal,  $\alpha^i = \sum_{j=0}^{n-1} a_{ij} x_j$  with  $a_{ij} \in \mathbb{Z}_{(p)}$ , and therefore  $[(O_K)_{(p)} : \mathbb{Z}_{(p)}[\alpha]] = |\det(a_{ij})|$ .

On the other hand,  $\text{Ind}(\alpha) = [O_K : \mathbb{Z}[\alpha]] = [(O_K)_{(p)} : (\mathbb{Z}[\alpha])_{(p)}] = [(O_K)_{(p)} : \mathbb{Z}_{(p)}[\alpha]]$ , hence  $(O_K)_{(p)} = \mathbb{Z}_{(p)}[\alpha]$  if and only if  $p$  does not divide  $\text{Ind}(\alpha)$  if and only if  $\text{Ind}(\alpha) \in \cup(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)} - p\mathbb{Z}_{(p)}$ . Hence by the proof of [Theorem 2.5](#),  $p$  does not divide  $\text{Ind}(\alpha)$  if and only if  $(\tilde{P}_i, \tilde{T}) = 1$  in  $\mathbb{F}_p[X]$  for every  $i = 1, 2, \dots, r$  (in other words, if and only if  $(\tilde{f}, \tilde{T}) = 1$  in  $\mathbb{F}_p[X]$ ).

(ii) $\Leftrightarrow$ (iii). By [\[2, Corollary 2, page 73\]](#),  $(\tilde{f}, \tilde{T}) = 1$  in  $\mathbb{F}_p[X]$  if and only if  $\text{Res}(\tilde{f}, \tilde{T}) = \overline{\text{Res}}(f, T) \neq \bar{0}$  in  $\mathbb{F}_p$  if and only if  $\text{Res}(f, T) \in \mathbb{Z} - p\mathbb{Z}$ . On the other hand,

$$\text{Res}(f, T) = \frac{(-1)^{\deg(f)}}{p^{\deg(f)}} \text{Res}(f, P). \tag{3.1}$$

(ii) $\Leftrightarrow$ (iv). We have  $(\tilde{f}, \tilde{T}) = 1$  in  $\mathbb{F}_p[X]$  if and only if  $\text{Res}(f, T) \in \mathbb{Z} - p\mathbb{Z}$ . On the other hand,  $\text{Res}(f, T) = \prod_{i=1}^r \text{Res}(P_i, T)$  and

$$\text{Res}(P_i, T) = \frac{(-1)^{\deg(P_i)}}{p^{\deg(P_i)}} \text{Res}(P_i, P). \tag{3.2}$$

□

**THEOREM 3.3.** *Let  $K = \mathbb{Q}(\alpha)$  be a number field of degree  $n$ ,  $P(X) \in \mathbb{Z}[X]$  a monic minimal polynomial of  $\alpha$ , and  $O_K$  the ring of integers of  $K$ . Assume  $\tilde{P}(X) = \prod_{i=1}^r \tilde{P}_i^{e_i}(X)$  in  $\mathbb{F}_p[X]$ , for every prime number  $p$  such that  $p^2$  divides  $\text{Disc}(P)$ , with  $P_i(X) \in \mathbb{Z}[X]$  a monic lifting of  $\tilde{P}_i(X)$  and  $e_i \geq 2$  for  $1 \leq i \leq r$ . Then  $O_K = \mathbb{Z}[\alpha]$  if and only if for every prime number  $p$ , such that  $p^2$  divides  $\text{Disc}(P)$ ,  $v_p(\text{Res}(P_i, P)) = \deg(P_i)$  for  $1 \leq i \leq r$ .*

**PROOF.** It suffices to apply [Propositions 3.1](#) and [3.2](#), and [Theorem 2.5](#). □

**REMARK 3.4.** [Proposition 3.2](#) provides a complement to the Dedekind criterion (see [\[4, page 305\]](#)). Indeed, in  $\mathbb{F}_p[X]$ , we have  $(\tilde{f}, \tilde{T}) = (\tilde{f}, \tilde{T}, \tilde{h})$  since all  $e_i \geq 2$ .

We finish this section giving other conditions equivalent to  $p$  not being a divisor of  $\text{Ind}(\alpha)$ .

**PROPOSITION 3.5.** *The following statements are equivalent:*

- (i)  $p$  does not divide  $\text{Ind}(\alpha) = [O_K : \mathbb{Z}[\alpha]]$ ;
- (ii)  $\mathbb{Z}[\alpha] + pO_K = O_K$ ;
- (iii)  $\mathbb{Z}[\alpha] \cap pO_K = p\mathbb{Z}[\alpha]$ .

**PROOF.** (ii) $\Leftrightarrow$ (iii). Consider the following map of  $\mathbb{F}_p$ -vector spaces:

$$j : \mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha] \rightarrow O_K/pO_K, \quad j(x + p\mathbb{Z}[\alpha]) = x + pO_K. \tag{3.3}$$

As  $O_K$  and  $\mathbb{Z}[\alpha]$  are two free groups of the same rank  $n$ ,  $\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]$  and  $O_K/pO_K$  are two  $\mathbb{F}_p$ -vector spaces of the same dimension  $n$  and injectivity of  $j$  is equivalent to surjectivity of  $j$ . Moreover,  $j$  is one-to-one if and only if  $\mathbb{Z}[\alpha] \cap pO_K = p\mathbb{Z}[\alpha]$  and  $j$  is onto if and only if  $\mathbb{Z}[\alpha] + pO_K = O_K$ .

(i)⇔(iii). If  $p$  does not divide  $\text{Ind}(\alpha)$  and  $p\mathbb{Z}[\alpha] \subset \mathbb{Z}[\alpha] \cap pO_K$ , then there exists  $x \in O_K$  such that  $x \notin \mathbb{Z}[\alpha]$  and  $px \in \mathbb{Z}[\alpha]$ , so the order of the subgroup generated by  $x + \mathbb{Z}[\alpha]$  of the finite group  $O_K/\mathbb{Z}[\alpha]$  is equal to  $p$ , and, by Lagrange’s theorem,  $p$  divides  $\text{Ind}(\alpha)$ , which is the order of the group  $O_K/\mathbb{Z}[\alpha]$ , and this is impossible.

Conversely, assume that  $\mathbb{Z}[\alpha] \cap pO_K = p\mathbb{Z}[\alpha]$  and  $p$  divides  $\text{Ind}(\alpha)$ . Cauchy’s theorem implies that there exists an element of order  $p$  in  $O_K/\mathbb{Z}[\alpha]$ ; in other words, there exists  $x \in O_K$  such that  $x \notin \mathbb{Z}[\alpha]$  and  $px \in \mathbb{Z}[\alpha]$ . Then  $px \in \mathbb{Z}[\alpha] \cap pO_K = p\mathbb{Z}[\alpha]$ , hence  $x \in \mathbb{Z}[\alpha]$ , which is impossible. □

### 4. Applications

#### 4.1. Monogenicity of cyclotomic fields

**PROPOSITION 4.1.** *Let  $n \geq 3$  be an integer,  $\xi_n$  a primitive  $n$ th root of unity,  $K = \mathbb{Q}(\xi_n)$ , and  $\phi_n(X)$  the  $n$ th cyclotomic polynomial over  $\mathbb{Q}$ . Then  $O_K = \mathbb{Z}[\xi_n]$ .*

**PROOF.** We know from [15] that

$$\begin{aligned} \phi_n(X) &= \prod_{\substack{1 \leq i \leq n \\ i \wedge n = 1}} (X - \xi_n^i) = \text{Irrd}(\xi_n, \mathbb{Q}), \\ \text{Disc}(\phi_n) &= (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}} = (-1)^{\varphi(n)/2} \prod_{i=1}^s p_i^{\varphi(n)(r_i-1/(p_i-1))}, \end{aligned} \tag{4.1}$$

where  $\varphi(n)$  is the Euler  $\varphi$ -function and

$$n = \prod_{i=1}^s p_i^{r_i} = p_i^{r_i} m_i \quad \text{with} \quad m_i = \prod_{j=1, j \neq i}^s p_j^{r_j}. \tag{4.2}$$

Let  $q$  be a prime number such that  $q^2$  divides  $\text{Disc}(\phi_n)$ . Then there exists  $i \in \{1, \dots, s\}$  such that  $q = p_i$ . We have  $\bar{\phi}_n(X) = (\bar{\phi}_{m_i}(X))^{\varphi(p_i^{r_i})} \pmod{p_i}$ , where  $\varphi(p_i^{r_i}) \geq 2$ , and

$$\text{Res}(\phi_{m_i}, \phi_n) = (-1)^{\varphi(m_i)\varphi(n)} \text{Res}(\phi_n, \phi_{m_i}) = \text{Res}(\phi_n, \phi_{m_i}) = p_i^{\varphi(m_i)}, \tag{4.3}$$

and we obtain that  $v_{p_i}(\text{Res}(\phi_n, \phi_{m_i})) = \text{deg}(\phi_{m_i}(X))$ .

Now the result follows immediately from [Theorem 3.3](#) and [Proposition 3.2](#). □

#### 4.2. Monogenicity of the field $K = \mathbb{Q}(\alpha)$ , with $\alpha$ a root of $P(X) = X^p - a$

**PROPOSITION 4.2.** *Let  $\alpha$  be a root of the irreducible polynomial  $P(X) = X^p - a$ , where  $a$  is a squarefree integer and  $p$  is a prime number.*



- (i) If  $p$  divides  $a$ , then  $O_K = \mathbb{Z}[\alpha]$  if and only if  $a$  is squarefree.
- (ii) If  $p$  does not divide  $a$ , then  $O_K = \mathbb{Z}[\alpha]$  if and only if  $a$  is squarefree and  $v_p(a^{p-1} - 1) = 1$ .

**PROOF.** We have  $P(X) = X^p - a = \text{Irrd}(\alpha, \mathbb{Q})$  and

$$\text{Disc}(P) = (-1)^{p((p-1)/2)} N_{K/\mathbb{Q}}(P'(\alpha)) = (-1)^{(3p^2-p-2)/2} p(ap)^{p-1}. \quad (4.4)$$

If  $p$  is odd, the only prime numbers  $q$  such that  $q^2$  divides  $\text{Disc}(P)$  are  $p$  and the prime divisors of  $a$ . If  $p = 2$ , then 2 is the only prime number  $q$  such that  $q^2$  divides  $\text{Disc}(P)$ .

Let  $q$  be a prime number such that  $q^2$  divides  $\text{Disc}(P)$ . We have two cases:

- (1) if  $q$  does not divide  $a$ , then  $\bar{P}(X) = \overline{g(X)}^p$  in  $\mathbb{F}_p[X]$ , with  $g(X) = X - a$ , and then  $\text{Res}(g, P) = P(a) = a^p - a$ ;
- (2) if  $q$  divides  $a$ , then  $\bar{P}(X) = \overline{g(X)}^p$  in  $\mathbb{F}_q[X]$ , with  $g(X) = X$  and then  $\text{Res}(g, P) = P(0) = -a$ .

In both cases, the result is deduced from [Theorem 3.3](#). □

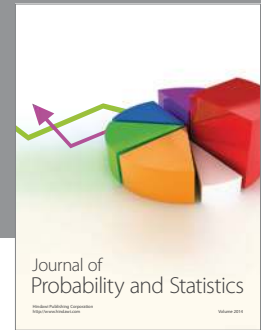
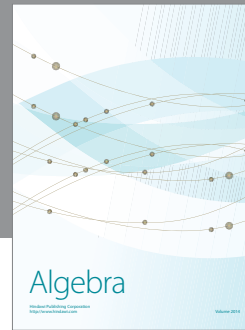
### REFERENCES

- [1] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Massachusetts, 1969.
- [2] N. Bourbaki, *Algèbre*, Masson, Paris, 1981.
- [3] M. Charkani, *Structure multiplicative des idéaux d'une extension primitive d'un anneau intégralement clos*, in preparation.
- [4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1996.
- [5] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Cyclotimy index*, Abh. Akad. Wiss. Göttingen Math.-Phys. Kl. **23** (1878), 1-23 (German).
- [6] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993.
- [7] M.-N. Gras, *Sur les corps cubiques cycliques dont l'anneau des entiers est monogène*, C. R. Acad. Sci. Paris Sér. A **278** (1974), 59-62 (French).
- [8] ———,  *$\mathbb{Z}$ -bases d'entiers  $1, \theta, \theta^2, \theta^3$  dans les extensions cycliques de degré 4 de  $\mathbb{Q}$  [ $\mathbb{Z}$ -bases of integers  $1, \theta, \theta^2, \theta^3$  in cyclic extensions of degree 4 of  $\mathbb{Q}$ ]*, Number Theory, Publ. Math. Fac. Sci. Besançon, Université de Franche-Comté, Besançon, 1981, pp. 1-14 (French).
- [9] ———, *Non monogénéité de l'anneau des entiers des extensions cycliques de  $\mathbb{Q}$  de degré premier  $l \geq 5$  [Nonmonogeneity of the ring of integers of cyclic extensions of  $\mathbb{Q}$  of prime degree  $l \geq 5$ ]*, J. Number Theory **23** (1986), no. 3, 347-353 (French).
- [10] G. J. Janusz, *Algebraic Number Fields*, Pure and Applied Mathematics, Academic Press, New York, 1973.
- [11] S. Lang, *Algebra*, 2nd ed., Addison-Wesley, Massachusetts, 1984.
- [12] P. Ribenboim, *Théorie des Valuations*, Les presses de l'université de Montréal, Montréal, 1964 (French).
- [13] P. Samuel, *Théorie Algébrique des Nombres*, Hermann, Paris, 1971 (French).

- [14] J.-P. Serre, *Corps Locaux*, Publications de l'Université de Nancago, Hermann, Paris, 1968 (French).
- [15] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982.

M. E. Charkani: Department of Mathematics, Faculty of Sciences Dhar-Mahraz, University of Sidi Mohammed Ben Abdellah, BP 1796, Fes, Morocco  
*E-mail address:* [mcharkani@excite.com](mailto:mcharkani@excite.com)

O. Lahlou: Department of Mathematics, Faculty of Sciences Dhar-Mahraz, University of Sidi Mohammed Ben Abdellah, BP 1796, Fes, Morocco  
*E-mail address:* [l.ouafae@caramail.com](mailto:l.ouafae@caramail.com)



# Hindawi

Submit your manuscripts at  
<http://www.hindawi.com>

